

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2005-252773

(P2005-252773A)

(43) 公開日 平成17年9月15日 (2005.9.15)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04 L 9/14	H04 L 9/00 641	5C025
H04 L 9/08	H04 N 5/44 A	5C063
H04 N 5/44	H04 N 7/16 Z	5C064
H04 N 7/08	H04 N 7/08 Z	5J104
H04 N 7/081	H04 L 9/00 601C	

審査請求 未請求 請求項の数 65 O L (全 24 頁) 最終頁に続く

(21) 出願番号 特願2004-61961 (P2004-61961)

(22) 出願日 平成16年3月5日 (2004.3.5)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(74) 代理人 100097445

弁理士 岩橋 文雄

(74) 代理人 100103355

弁理士 坂口 智康

(74) 代理人 100109667

弁理士 内藤 浩樹

(72) 発明者 森岡 芳宏

大阪府門真市大字門真1006番地 松下

電器産業株式会社内

(72) 発明者 綾木 靖

大阪府門真市大字門真1006番地 松下

電器産業株式会社内

最終頁に続く

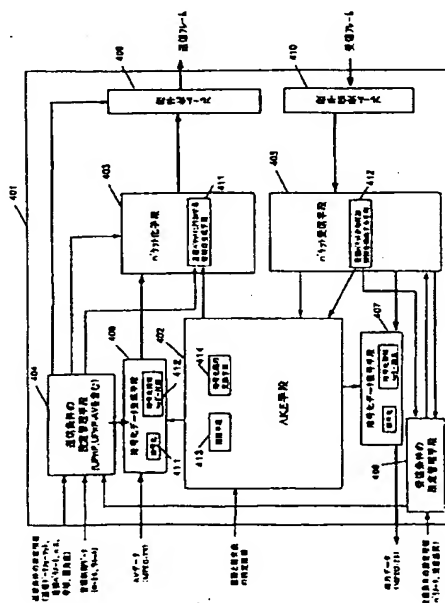
(54) 【発明の名称】 パケット送信機器

(57) 【要約】

【課題】 デジタル放送やDVDディスクなどの著作権保護されたMPEGなどのAVコンテンツを、そのフォーマット情報やコピー制御情報を継承しつつ、IPネットワーク上で秘匿性を守って伝送する手段を実現する。

【解決手段】 パケット送信手段は、AVデータと非AVデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、または、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加のいずれかを行う制御手段とを具備する。

【選択図】 図4



【特許請求の範囲】

【請求項 1】

パケット送信機器とパケット受信機器の間でデータのパケット通信を行なうパケット送受信システムにおけるパケット送信機器であって、

前記パケット送信機器は、

A Vデータと非 A Vデータとをそれぞれ入力するデータ入力手段と、

前記データ入力手段の出力を入力し、規定の送受信条件により、暗号化または暗号化情報ヘッダー付加の実行を行う暗号化データ生成手段と、

パケットヘッダー付加手段とを具備し、

前記暗号化データ生成手段は、認証処理を含む制御手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記非 A Vデータは前記 A Vデータのコピー制御情報、およびフォーマット情報を含み、前記コピー制御情報およびフォーマット情報より、前記暗号化手段において暗号化の制御、または、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかの制御の少なくとも一方の制御を行う手段とを具備するパケット送信機器。

10

【請求項 2】

前記暗号化データ生成手段内の前記暗号化手段は、暗号化に際して暗号化鍵を使用し、前記パケット送信機器と前記パケット受信機器が規定の条件を具備していることを検証し認証が行われた後に暗号化鍵が前記パケット送信機器と前記パケット受信機器で共有され、規定の伝送条件により前記暗号化鍵が更新されることを特徴とする請求項 1 記載のパケット送信機器。

20

【請求項 3】

前記暗号化鍵は、前記パケット送信機器が持っている暗号化鍵生成用の元データと、複数モードを持つ暗号化制御情報に対応した複数の暗号化鍵をメモリ空間に保持し、送信の暗号化モードが決定の後、前記複数の暗号化鍵よりその暗号化モードに応じた暗号化鍵を選択して暗号化手段の暗号化鍵を設定し、暗号化を行うことを特徴とする請求項 2 記載のパケット送信機器。

【請求項 4】

前記暗号化鍵生成用の元データは、機器またはデバイスの証明書、機器固有情報、外部から設定する鍵作成データの少なくとも一部の情報を含むことを特徴とする請求項 3 記載のパケット送信機器。

30

【請求項 5】

前記制御手段において、前記 A Vデータのコピー制御情報が、コピーフリーの場合には、前記 A Vデータのフォーマット情報を変更しないで前記 A Vデータに付加して前記パケット送信機器から前記パケット受信機器に伝送を行ない、また、前記 A Vデータのコピー制御情報がコピーフリー以外の場合には、前記 A Vデータのフォーマット情報を変更した後、前記 A Vデータを暗号化したデータに付加して前記パケット送信機器から前記パケット受信機器に伝送を行なうことを特徴とする請求項 2 記載のパケット送信機器。

【請求項 6】

前記 A Vデータのフォーマット情報は、M I M Eタイプ、ファイルタイプ、または拡張子のいずれかを含むことを特徴とする請求項 5 記載のパケット送信機器。

40

【請求項 7】

前記認証処理を含む制御手段において認証を実行するモードは、前記データ入力手段より入力される前記 A Vデータまたは前記非 A Vデータが含まれている制御情報により決定されることを特徴とする請求項 1 記載のパケット送信機器。

【請求項 8】

前記外部より入力される制御情報または認証用の T C Pポート情報は、コンテンツ毎にアクセス位置を指定する U R I、または、Q u e r yにより拡張された U R I 情報とにより与えられることを特徴とする請求項 7 記載のパケット送信機器。

【請求項 9】

50

前記外部より入力される制御情報または認証用のTCPポート情報は、コンテンツ毎にアクセス位置を指定するURIで要求されたコンテンツの情報の返信時に与えることを特徴とする請求項7記載のパケット送信機器。

【請求項10】

前記認証手段において認証を実行するモードは、

前記外部より入力される制御情報および前記入力AVデータの双方により決定することを特徴とする請求項3記載のパケット送信機器。

【請求項11】

前記前記暗号化情報ヘッダーは、暗号化モード情報と暗号化ペイロード長の少なくとも1つを含んでいることを特徴とする請求項1から10のいずれかに記載のパケット送信機器

10

【請求項12】

前記暗号化情報ヘッダーは、前記AVデータがコピーフリーコンテンツを放送する放送チャネルを受信したコンテンツの場合には付加しない、

また、前記AVデータが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信したコンテンツの場合には付加する、また、前記AVデータが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には付加しない、

また、前記AVデータが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には付加する、ことを特徴とする請求項11記載のパケット送信機器。

【請求項13】

前記コピーフリーコンテンツを放送する放送チャネルは、アナログ放送であるVHF、UHF、またはBSアナログ放送の放送チャネルであることを特徴とする請求項12記載のパケット送信機器。

20

【請求項14】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、およびEPNフラグ付きコピーフリーのうち少なくとも1つのモードを含んでいることを特徴とする請求項12記載のパケット送信機器。

【請求項15】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルは、デジタル放送であるBSデジタル放送、地上波デジタル放送、またはCSデジタル放送の放送チャネルであることを特徴とする請求項12記載のパケット送信機器。

30

【請求項16】

前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、前記放送の配信を行う事業者との間での認証手段により正当な受信機器または受信ユーザであることを認証された場合に行われることを特徴とする請求項15記載のパケット送信機器

【請求項17】

前記認証は、日本のデジタル衛星放送のB-CASカード、または米国のCATV放送で使用されるPODカードなどのセキュリティモジュールによる認証であることを特徴とする請求項16記載のパケット送信機器。

40

【請求項18】

前記暗号化手段は前記暗号化情報ヘッダーを、前記AVデータがフリーコンテンツの場合には付加しない、または、前記AVコンテンツの意味のあるデータ単位毎に付加することを特徴とする請求項1から10のいずれかに記載のパケット送信機器。

【請求項19】

AVデータと非AVデータとをそれぞれのデータバッファに入力し、前記2つのバッファの出力は優先制御して前記パケットヘッダー付加手段に出力することを特徴とする請求項1から18のいずれかに記載のパケット送信機器。

【請求項20】

50

前記優先制御の方法は、前記非 A V データが前記データバッファでオーバーフローしない様に制御しながら、前記 A V データを前記データバッファから優先して出力することを特徴とする請求項 19 記載の packets 送信機器。

【請求項 21】

前記前記 packets ヘッダー付加手段に出力は、あらかじめ決められた間隔値に対して一定のゆらぎ幅を持った概略一定間隔毎に出力する様に、packets シェーピングして出力することを特徴とする請求項 19 記載の packets 送信機器。

【請求項 22】

前記暗号化鍵を共有するための認証と鍵交換方式は、D T C P 方式であることを特徴とする請求項 1 から 21 のいずれかに記載の packets 送信機器。

10

【請求項 23】

前記暗号化鍵の I D 情報または更新情報として整数値を前記暗号化情報ヘッダーまたは packets ヘッダーに付加することを特徴とする請求項 22 記載の packets 送信機器。

【請求項 24】

packets ヘッダー付加手段から出力される packets を H T T P プロトコルで伝送する場合、H T T P packets の packets 毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項 23 記載の packets 送信機器。

【請求項 25】

packets ヘッダー付加手段から出力される packets を H T T P プロトコルで伝送する場合、T C P プロトコルが切断して再コネクションを張る毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項 23 記載の packets 送信機器。

20

【請求項 26】

前記暗号化モードの変化は T C P プロトコルまたは U D P プロトコルのポート番号の変化で検出して設定することを特徴とする請求項 22 記載の packets 送信機器。

【請求項 27】

前記暗号化モードの情報を packets 内に持つことを特徴とする請求項 22 記載の packets 送信機器。

【請求項 28】

前記 A V データの packets 化は、R T P、U D P、I P プロトコルで行うことを特徴とする請求項 1 から 27 のいずれかに記載の packets 送信機器。

30

【請求項 29】

前記暗号化鍵の更新条件としては、あらかじめ決められた時間ごとに行うという条件も用いることを特徴とする請求項 28 記載の packets 送信機器。

【請求項 30】

前記 A V データの packets 化は、ハードウェアで行うことを特徴とする請求項 28 記載の packets 送信機器。

【請求項 31】

マルチキャスト伝送の場合、前記暗号化上布ヘッダーを付加した packets と付加しない packets の両方を出力することを特徴とする請求項 28 記載の packets 送信機器。

40

【請求項 32】

前記 A V データを前記 R T P、U D P、I P プロトコルによる I P packets 化の前に、フォワードエラーコレクション (F E C) による誤り訂正を付加することを特徴とする請求項 28 記載の packets 送信機器。

【請求項 33】

前記フォワードエラーコレクション (F E C) はリードソロモン方式またはパリティ方式であることを特徴とする請求項 28 記載の packets 送信機器。

【請求項 34】

前記暗号化情報ヘッダーを付加する場合は、前期 R T P プロトコルにおいて定義されているマーカービット (M ビット) を有効状態にアサートすることを特徴とする請求項 28 記

50

載のパケット送信機器。

【請求項 3 5】

前記 A V データのパケット化は、H T T P、T C P、I P プロトコルで行うことを特徴とする請求項 1 から 2 7 のいずれかに記載のパケット送信機器。

【請求項 3 6】

前記暗号化鍵の更新条件としては、あらかじめ決められた時間ごとに行うという条件も用いることを特徴とする請求項 3 5 記載のパケット送信機器。

【請求項 3 7】

前記認証モードでは前記 H T T P ヘッダーに、認証モード情報を付加することを特徴とする請求項 3 5 記載のパケット送信機器。

10

【請求項 3 8】

前記 A V データのパケット化は、受信側からの制御により R T P または H T T P プロトコルで行うことを切替え制御することを特徴とする請求項 1 から 3 6 記載のパケット送信機器。

【請求項 3 9】

前記 A V データのパケット化は、受信側でのチャンネル選択時には受信側からの制御により R T P プロトコルを用いて行ない、受信チャンネルが確定した後に H T T P プロトコルを用いて行う様に切り替え制御することを特徴とする請求項 3 8 記載のパケット送信機器。

【請求項 4 0】

前記 A V データのパケット化は、受信側の A V データ出力が表示ディスプレイに対して出力されており蓄積されない場合は R T P を用い、また、受信側の A V データ出力が記録メディアに蓄積される場合は H T T P を用いる様に、切替え制御することを特徴とする請求項 3 8 記載のパケット送信機器。

20

【請求項 4 1】

前記 A V データは、S M P T E 2 5 9 M 規格で規定された非圧縮 S D 方式信号、または、S M P T E 2 9 2 M 規格で規定された非圧縮 H D 形式、または、I E C 6 1 8 8 3 規格で規定された I E E E 1 3 9 4 による D V またはデジタル放送の M P E G - T S の伝送ストリーム形式、または、D V B 規格 A 0 1 0 で規定された D V B - A S I による M P E G - T S 形式、または、M P E G - P E S、M P E G - E S、M P E G 4、I S O / I E C H. 2 6 4 の内のいずれか一つのデータストリーム形式を含むことを特徴とする請求項 2 8 から 4 0 のいずれかに記載のパケット送信機器。

30

【請求項 4 2】

前記 A V データを構成するデータブロックに時間情報を付加し、1 つ以上の時間情報付データブロックをまとめて R T P または H T T P 上にマッピングすることを特徴とする請求項 4 1 記載のパケット送信機器。

【請求項 4 3】

前記時間情報としては、送信側の規定条件によりタイムスタンプ又は定型値データを選択して用いることを特徴とする請求項 4 2 記載のパケット送信機器。

【請求項 4 4】

M I M E タイプ、ファイルタイプ、または拡張子のいずれかを含む前記 A V データのフォーマット情報をタイムスタンプ付加の判別条件に用いて、前記送信側でタイムスタンプが付加できる場合には、前記タイムスタンプを用いることを特徴とする請求項 4 3 記載のパケット送信機器。

40

【請求項 4 5】

前記 A V データは、M P E G - T S であることを特徴とする請求項 4 2 記載のパケット送信機器。

【請求項 4 6】

前記各 T S パケットに付加するタイムスタンプのクロックは M P E G のシステムクロック周波数に等しいことを特徴とする請求項 4 3 記載のパケット送信機器。

【請求項 4 7】

50

前記TSパケットに付加された時間情報がタイムスタンプの場合、MPEG-TSのネットワーク伝送により前記各TSパケットに重畳されたジッターを受信側のシステムクロック値と前記書くTSパケットのタイムスタンプの差分を一定にすることで伝送された前記書くTSパケットの伝送ジッターを除去して、受信側で前記TSパケットに含まれるPCRを用いてMPEGシステムクロックの再生を行うことを特徴とする請求項46記載のパケット送信機器。

【請求項48】

前記TSパケットに付加された時間情報が定型値データの場合、受信したMPEG-TSは送信時の時刻情報を用いずにMPEGデコードを行うことを特徴とする請求項46記載のパケット送信機器。

10

【請求項49】

Nを2以上の整数とした場合、UDPプロトコルまたはTCPプロトコルのN個のポートを用いて、N個のフォーマットのAVデータをそれぞれのポート毎に割り当てて伝送することを特徴とする請求項41記載のパケット送信機器。

【請求項50】

UDPプロトコルまたはTCPプロトコルの単一のポートを用いて、複数のフォーマットのAVデータを多重して伝送することを特徴とする請求項41記載のパケット送信機器。

【請求項51】

Nを2以上の整数、また、MをNより大きい整数とした場合、UDPプロトコルまたはTCPプロトコルのM個のポートを用いて、N個のフォーマットのAVデータを単一または多重してM個のポートに割り当てて伝送することを特徴とする請求項41記載のパケット送信機器。

20

【請求項52】

複数のAVデータを同時に伝送する場合、高データレートのAVデータはUDPプロトコルで伝送し、低データレートのAVデータはTCPプロトコルで伝送することを特徴とする請求項41記載のパケット送信機器。

【請求項53】

複数のAVデータを同時に伝送する場合、高データレートのAVデータより、低データレートのAVデータを優先して伝送することを特徴とする請求項41記載のパケット送信機器。

30

【請求項54】

前記AVデータの伝送範囲を制限することを特徴とする請求項1から53のいずれかに記載のパケット送信機器。

【請求項55】

前記AVデータの伝送範囲の制限は、IPプロトコルのTTL(Time to Live)の値を用いて制限することを特徴とする請求項54記載のパケット送信機器。

【請求項56】

前期前記AVデータの伝送範囲を制限は、IPパケットのRTT(Round Trip Time)の値を用いて制限することを特徴とする請求項54記載のパケット送信機器。

40

【請求項57】

前記AVデータの伝送範囲を制限は、MAC層のヘッダー情報により制限することを特徴とする請求項54記載のパケット送信機器。

【請求項58】

前記IPパケットのパケットサイズは前記送信手段と前記受信手段の中間に位置するIPネットワークのパスMTUサイズ以下に設定することを特徴とする請求項1から57のいずれかに記載のパケット送信機器。

【請求項59】

前記IPパケットの伝送は、IEEE 802.3で規定された伝送方法により行われることを特徴とする請求項1から57のいずれかに記載のパケット送信機器。

50

【請求項60】

前記IPパケットの伝送は、IEEE 802.11で規定された伝送方法により行われることを特徴とする請求項1から57のいずれかに記載のパケット送信機器。

【請求項61】

前記IEEE 802.11の使用において、WEPまたはWPAまたはその他のネットワーク接続制限手段を用いることを特徴とする請求項60記載のパケット送信機器。

【請求項62】

前記IPパケットの伝送は、IEEE 802.1Qにより規定された伝送方法により行われることを特徴とする請求項1から57のいずれかに記載のパケット送信機器。

【請求項63】

前記IPパケットの伝送は、IPバージョン4、または、IPバージョン6を使用して行われることを特徴とする請求項1から57記載のパケット送信機器。

【請求項64】

前記IPバージョン4を用いる場合、TOSフィールドを用いて優先制御を行なうことを特徴とする請求項63記載のパケット送信機器。

【請求項65】

前記IPバージョン6を用いる場合、Priorityフィールドを用いて優先制御を行なうことを特徴とする請求項63記載のパケット送信機器。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、IEEE 802.3などのイーサネット(R)(有線LAN)やIEEE 802.11などの無線LANなどを用いて、暗号化されたAVストリームをIPパケット化して高品質に送信するパケット送信機器に関する。

【背景技術】

【0002】

従来、一般家庭において、IEEE 1394を用いて、IEC 61883-4で規定された方式に基づきMPEG-TS信号の暗号化伝送が行なわれている。MPEG-TSなどAVデータを暗号化して伝送する方式の一例として、DTCP(Digital Transmission Content Protection)方式が規定されている。DTCPは、IEEE 1394やUSBなどの伝送メディア上のコンテンツ保護技術である。DTCP方式は、DTLA(Digital Transmission Licencing Administrator)で規格化された方式であり、<http://www.dtcp.com>、http://www.dtcp.com/data/dtcp_tut.pdf、http://www.dtcp.com/data/wp_spec.pdfや、書籍「IEEE 1394、AV機器への応用」、高田信司監修、日刊工業新聞社、「第8章、コピープロテクション」(133~149ページ)で説明されている。

【0003】

図12は、DTCP方式を用いたMPEG-TSのIEEE 1394での伝送の一例である。DTCP方式では、送信側をソース(1801)、受信側をシンク(1802)と呼び、暗号化したMPEG-TSなどのコンテンツをソース(1801)からネットワーク(1803)を介して、シンク(1802)へ伝送している。図12に、補足情報として、ソース機器およびシンク機器の例を併記する。

【0004】

次に、図13を用いて、DTCP方式における従来のパケット通信手段の概略を説明する。図13は図12のソース(1801)、およびシンク(1802)の構成の概略図である。まず、DTCP方式に準拠した認証と鍵交換(Authentication and Key Exchange、AKEと略する)が行なわれる。AKE手段(1901)に対して、その認証と鍵交換設定情報が入力され、この情報がパケット化手段(1902)により規定のヘッダーを付加されパケット化され、ネットワーク(1907)に出力される。ここで、パケット化手段(1902)は送信条件設定手段(1903)により決定された送信パラメータにより、入力データのパケット化および送信を行なう。受信側では、ネットワーク(1907

より入力する信号がパケット受信手段(1904)でパケットヘッダーなどの識別によりフィルタリングされ、AKE手段(1901)に入力される。これにより送信側(ソース)のAKE手段と、受信側(シンク)のAKE手段がネットワーク(1803、1907)を介してお互いにメッセージの通信ができる。すなわち、D T C P方式の手順に従い、認証と鍵交換を実行する。

【0005】

送信側(ソース)と、受信側(シンク)で認証と鍵交換が成立すれば、次に、A Vデータの伝送を行なう。ソースでは、M P E G - T S信号を暗号化データ生成手段(1905)に入力して、M P E G - T S信号を暗号化した後、この暗号化されたM P E G - T S信号をパケット化手段(1902)に入力し、ネットワーク(1907)に出力する。シンクでは、ネットワーク(1907)より入力する信号がパケット受信手段(1904)でパケットヘッダーなどの識別によりフィルタリングされ、暗号化データ復号手段(1906)に入力され、復号されM P E G - T S信号が出力される。

【0006】

次に、図14を用い上記手順を補足説明する。図14において、ソースとシンク間はI E E E 1394で接続されている。まず、ソース側でコンテンツの送信要求が発生する。そして、ソースからシンクへ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。シンクは、コンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。ソースとシンクはD T C P所定の処理により認証鍵(Kauth)の共有を図る。そして、ソースは認証鍵を用いて交換鍵(Kx)を暗号化してシンクに送り、シンクで交換鍵(Kx)が復号される。ソースでは暗号鍵(Kc)を時間的に変化させるために、時間的に変化するシード情報(Nc)を生成し、シンクに送信する。ソースでは、交換鍵(Nx)とシード情報(Nc)より暗号化鍵(Kx)を生成して、M P E G - T Sをこの暗号化鍵を用いて暗号化手段で暗号化してシンクに送信する。シンクはシード情報を受信し交換鍵とシード情報情報より復号鍵を復元する。シンクではこの復号鍵を用いて暗号化されたM P E G - T S信号を復号する。

【0007】

図15は、図12においてM P E G - T S信号を伝送する場合のI E E E 1394アイソクロナスパケットの一例である。このパケットは、4バイト(32ビット)のヘッダー、4バイト(32ビット)のヘッダーCRC、224バイトのデータフィールド、4バイト(32ビット)のトレイラによって構成されている。暗号化されて伝送されるのは224バイトのデータフィールドを構成するC I PヘッダーとT S信号のうち、T S信号のみで、他のデータは暗号化されない。ここで、D T C P方式固有の情報は、コピー保護情報である2ビットのE M I (Encryption Mode Indicator)、および1ビットのシード情報O / E (Odd/Even)であり、これらは上記32ビットのヘッダー内に存在するため暗号化されずに伝送される。

【特許文献1】特開2004-56776号公報

【非特許文献1】「I E E E 1394、A V機器への応用」、高田信司監修、日刊工業新聞社、「第8章、コピープロテクション」(133~149ページ)

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、上記従来の構成では以下のような問題点を有していた。従来のD T C P方式はI E E E 1394において、アイソクロナスパケットを用いて伝送するためM P E G - T S信号のリアルタイム伝送ができるが、インターネットの標準プロトコルであるI Pプロトコルを用いて、イーサネット(R)(I E E E 802.3)、無線L A N (I E E E 802.11)や、その他のI Pパケットを伝送可能なネットワークで伝送ができないという大きな問題点がある。すなわち、I Pプロトコルを介して論理的に接続された送信機器と受信機器の間を、暗号化によりコンテンツの機密性や著作権の保護を行なった状態でM P E G - T S信号などA Vストリームを伝送できないという大きな問題点が

10

20

30

40

50

ある。

【課題を解決するための手段】

【0009】

上記課題を解決するために、本願第1の発明は、AVデータと非AVデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件、すなわち、AVデータのコピー制御情報、およびフォーマット情報により、暗号化または暗号化情報ヘッダー付加の実行を行う暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送信機器において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、または、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかの少なくとも共いづれか一方を制御する手段とを具備する。これにより、MPEG-TS信号などのAVストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダーを付加を決めることにより、送受信機器間での信号の互換性を確保しながら、AVストリームの秘匿性を保つこと、すなわち、コンテンツの著作権を保護することが可能となる。

10

【0010】

本願第2の発明は、第1の発明における暗号化手段におけるAVデータ伝送中の鍵更新において、複数の暗号化鍵から1つの暗号化鍵を選択して暗号化処理を高速実行するために、暗号化鍵はパケット送信機器が持っている暗号化鍵生成用の元データと、複数モードを持つ暗号化制御情報に対応した複数の暗号化鍵をメモリ空間に保持し、送信の暗号化モードが決定の後、複数の暗号化鍵よりその暗号化モードに応じた暗号化鍵を選択して暗号化手段の暗号化鍵を設定し、暗号化を行う。これらの構成により、高速なAVデータを伝送しながら、複数の暗号化鍵から1つの暗号化鍵を選択して鍵更新を高速に行いながら、暗号化処理を高速実行することが可能となる。

20

本願第3の発明は、第1の発明における暗号化データ生成手段において、外部入力されるAVストリームのコピー制御情報(CCI)に従うより、MIME-TYPEなどAVデータのフォーマット情報を暗号化データ仕様のフォーマットに変更をした後、暗号化伝送する。さらに、AVストリームのオリジナルのフォーマット情報をUPnP-AV方式や独自の通信方式を利用して別のデータにマッピングして、送信側から受信側に伝送する。これらの構成により、AVデータのフォーマット情報を変更して暗号化伝送しながら、受信側でAVデータのオリジナルのフォーマット情報を復元することが可能となる。

30

本願第4の発明は、第1の発明において、AVデータのパケット化は、受信側からの制御により、RTP/UDPまたはHTTP/TCPプロトコルの切替え制御を、きめ細かく、かつ映像の途切れなくスムーズに行う。たとえば、AVデータのパケット化は、受信側から送信側におけるTVチューナのチャンネル選択や、受信側でHDDがDVDディスクに録画されたAVコンテンツの選択を行う場合には、伝送遅延の小さいRTP/UDPプロトコルを用い、TVチューナのチャンネル選択や録画されたAVコンテンツの選択を速く行うことができる。また、これらの視聴コンテンツ選択が終了した後は、HTTP/TCPプロトコルを用い、RTP/UDPよりもパケット落ちに対してTCPでの再送機能を持つHTTP/TCP方式を用いて高画質なコンテンツ視聴を行う。これらの構成により、切替え制御することにより受信側でコンテンツ選択をする場合は低遅延でユーザに遅延を感じさせない軽快な操作が可能となり、また、視聴コンテンツ選択が終了した後はパケットロスなどによる信号欠落が補償された高品質なAVコンテンツの伝送が可能となる。

40

本願第5の発明は、第1の発明において、AVデータを構成するデータブロックに、タイムスタンプまたは提携データから構成される時間情報を付加し、時間情報を付加した付データブロックを1つ以上まとめてRTPパケットのペイロード部またはHTTPパケットのペイロード部にマッピングする。これにより、TSパケットにタイムスタンプや特定情報を付加できるので、受信側でMPEG-TSのデコードをタイムスタンプを用いて行うか、タイムスタンプを用いないで用いるかをきめ細かく制御することが可能となる。

【発明の効果】

50

【0011】

本願第1の発明によれば、以下のような効果を有する。すなわち、本願第1の発明によるパケット送信手段は、A Vデータと非A Vデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件、すなわち、A Vデータのコピー制御情報、およびフォーマット情報により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしつか、または、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかの少なく共いづれか一方を制御する手段とを具備する。これにより、M P E G - T S 信号などのA Vストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダーを付加を決めることにより、送受信機器間での信号の互換性を確保しながら、A Vストリームの秘匿性を保つこと、すなわち、コンテンツの著作権を保護することが可能となる。

10

本願第2の発明によれば、以下のような効果を有する。すなわち、本願第2の発明によるパケット送信手段は、第1の発明における暗号化手段におけるA Vデータ伝送中の鍵更新において、複数の暗号化鍵から1つの暗号化鍵を選択して暗号化処理を高速実行するために、暗号化鍵は送信手段が持っている暗号化鍵生成用の元データと、複数モードを持つ暗号化制御情報に対応した複数の暗号化鍵をメモリ空間に保持し、送信の暗号化モードが決定の後、複数の暗号化鍵よりその暗号化モードに応じた暗号化鍵を選択して暗号化手段の暗号化鍵を設定し、暗号化を行う。これらの構成により、高速なA Vデータを伝送しながら、複数の暗号化鍵から1つの暗号化鍵を選択して鍵更新を高速に行いながら、暗号化処理を高速実行することが可能となる。

20

本願第3の発明によれば、以下のような効果を有する。本願第3の発明は、第1の発明における暗号化データ生成手段において、外部入力されるA Vストリームのコピー制御情報(C C I)に従うより、M I M E - T Y P E などA Vデータのフォーマット情報を暗号化データ仕様のフォーマットに変更をした後、暗号化伝送する。さらに、A Vストリームのオリジナルのフォーマット情報をU P n P - A V方式や独自の通信方式を利用して別のデータにマッピングして、送信側から受信側に伝送する。これらの構成により、A Vデータのフォーマット情報を変更して暗号化伝送しながら、受信側でA Vデータのオリジナルのフォーマット情報を復元することが可能となる。

30

本願第4の発明によれば、以下のような効果を有する。本願第4の発明は、第1の発明において、A Vデータのパケット化は、受信側からの制御により、R T P / U D P または H T T P / T C P プロトコルの切替え制御を、きめ細かく、かつ映像の途切れなくスムーズに行う。たとえば、A Vデータのパケット化は、受信側から送信側におけるT Vチューナのチャンネル選択や、受信側でH D DがD V Dディスクに録画されたA Vコンテンツの選択を行う場合には、伝送遅延の小さいR T P / U D P プロトコルを用い、T Vチューナのチャンネル選択や録画されたA Vコンテンツの選択を速く行うことができる。また、これらの視聴コンテンツ選択が終了した後は、H T T P / T C P プロトコルを用い、R T P / U D P よりもパケット落ちに対してT C Pでの再送機能を持つH T T P / T C P方式を用いて高画質なコンテンツ視聴を行う。これらの構成により、切替え制御することにより受信側でコンテンツ選択をする場合は低遅延でユーザに遅延を感じさせない軽快な操作が可能となり、また、視聴コンテンツ選択が終了した後はパケットロスなどによる信号欠落が補償された高品質なA Vコンテンツの伝送が可能となる。

40

本願第5の発明によれば、以下のような効果を有する。すなわち、本願第5の発明は、第1の発明において、A Vデータを構成するデータブロックに、タイムスタンプまたは提携データから構成される時間情報を付加し、時間情報を付加した付データブロックを1つ以上まとめてR T P パケットのペイロード部またはH T T P パケットのペイロード部にマッピングする。これにより、T S パケットにタイムスタンプや特定情報を付加できるので、受信側でM P E G - T S のデコードをタイムスタンプを用いて行うか、タイムスタンプを

50

用いないで用いるかをきめ細かく制御することが可能となる。

また、本願第1から第5までの発明によれば、ネットワークを用いたA Vコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ(A Vデータコンテンツ)の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるA Vデータの販売、課金が可能となり、安全性の高いB-B、B-Cのコンテンツ販売流通が可能となる。

また、本願第2から第65での発明によれば、A Vコンテンツをハードウェアで伝送処理する場合にも、一般のデータパケットは従来通りCPUを用いてソフトウェア処理を行える。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データであるA Vデータに比べて非常に少ないので、マイコンなど安価なマイクロプロセッサで実現可能となり低コストで実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なCPUや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できるという大きなメリットがある。

【発明を実施するための最良の形態】

【0012】

まず最初に本願発明の位置付けを明確にするために適用されるシステム例の概略について説明する。図1は本願発明を適用するシステムの一例である。

図1において、パケット送信機器(101)およびパケット受信機器(103)は、本願第1、2、3、4および5の発明実施部である(以下、本願発明部)。101は送信機器、102はルータ、103は受信機器である。送信機器(101)には、送受信条件の設定情報、認証と鍵交換の設定情報、入力ストリーム(MPEG-TSなどコンテンツ)が入力され、以下の手順1から3に基づき、通信が実行される。

手順1) 送受信パラメータの設定を行なう。

(1-1) 送受信機器のMACアドレス、IPアドレス、TCP/UDPポート番号等を設定。

(1-2) 送信信号フォーマットの種別、帯域を設定。QoSエージェントとして動作する送信機器(101)と受信機器(103)、QoSマネージャとして動作するルータ(102)との間でIEEE 802.1Q(VLAN)規格を用いたネットワークの運用に関する設定を実施。

(1-3) 優先度の設定(IEEE 802.1Q/pによる運用)

手順2) 認証と鍵交換：

(2-1) 認証と鍵交換を行なう。たとえば、DTCP方式を用いることもできる。

手順3) ストリーム伝送：

(3-1) 送信機器と受信機器間での暗号化されたストリームコンテンツ(MPEG-TS)の伝送
なお、コンテンツの入力信号として、例ではMPEG-TSを使用しているが、これに限らず本発明で用いる入力コンテンツの適用範囲としては、MPEG1/2/4などMPEG-TSストリーム(ISO/IEC 13818)、DV(IEC 61834、IEC 61883)、SMPTE 314M(DV-based)、SMPTE 259M(SDI)、SMPTE 305M(SDT1)、SMPTE 292M(HD-SDI)等で規格化されているストリームなお、一般的なA Vコンテンツも適用可能である。さらに、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、データ転送速度がコンテンツストリームの通常再生データレートよりも大きくなるなどの条件化において、リアルタイムより高速のコンテンツ伝送も可能である。

次に、上記手順2の認証と鍵交換に関して補足説明する。図2において、送信機器と受信機器間はIPネットワークにより接続されている。まず、送信機器から受信機器へコンテンツのコピー保護情報を含んだコンテンツの保護モード情報が送信される。受信機器は、コンテンツのコピー保護情報の解析を行い、使用する認証方式を決定して認証要求を送信

10

20

30

40

50

機器に送る。これらの処理を通して送信機器と受信機器は認証鍵を共有する。次に、送信機器は認証鍵を用いて交換鍵を暗号化して受信機器に送り、受信機器で交換鍵が復号される。送信機器では暗号鍵を時間的に変化させるために、時間的に変化する鍵変更情報を生成し、受信機器に送信する。送信機器では、交換鍵と鍵変更情報より暗号化鍵を生成して、MPEG-TSをこの暗号化鍵を用いて暗号化手段で暗号化して受信機器に送信する。受信機器は受信した鍵変更情報を交換鍵より復号鍵を復元する。受信機器ではこの復号鍵を用いて暗号化されたMPEG-TS信号を復号する。

図3は本方式をイーサネット(R)を用い2階建ての家庭に適用した場合の一例である。図3において、301は1階のネットワーク構成、302は2階のネットワーク構成である。303は1階に設置されインターネットと接続されるルータ、304は2階に設置されているスイッチングハブである。304はルータ(303)とスイッチングハブ(304)を接続するイーサネット(R)ネットワークである。家庭内の全てのイーサネット(R)ネットワークの帯域は100Mbpsである。1階のネットワーク構成の詳細としては、ルータ(303)にはテレビ(TV)、パソコン(PC)、DVDレコーダが100Mbpsのイーサネット(R)で接続され、また、エアコン、冷蔵庫がECHONETで接続されている。また、2階では、スイッチングハブ(304)にテレビ(TV)、パソコン(PC)、DVDレコーダが100Mbpsのイーサネット(R)で接続され、また、エアコンがECHONETで接続されている。なお、ECHONETは「エコーネットコンソーシアム」(<http://www.echonet.gr.jp/>)で開発されている伝送方式である。

図3において、パソコン(PC)、DVDレコーダ、ルータ(301)およびスイッチングハブ(304)は、IEEE 802.1Q(VLAN)に対応している。すなわち、ルータ(301)およびスイッチングハブ(304)において、各ポートのデータレートが全て同じ(例えば100Mbps)場合、特定ポートへ出力されるデータ帯域の合計がそのポートの伝送レートの規格値または実力値を超えない限り、入力ポートへ入力されたデータはルータ(あるいは、スイッチングハブ)内部で失われず全て出力ポートに出力される。スイッチングハブでは、たとえば8個の入力ポートにデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれのデータはハブ内部のバッファで競合しないでスイッチングされて出力ポートより出力されるため、入力データはパケット落ちすることなく全て出力ポートに出力される。

図3において、家庭内の全てのイーサネット(R)の帯域が100Mbpsであるため、1階と2階間のネットワーク305の帯域も100Mbpsである。1階と2階の複数の機器間で複数のデータが流れる場合、各データに対する帯域制限がない場合、このネットワーク305上を流れるデータのデータレート合計が100Mbpsを超える可能性があり、MPEG-TSの映像アプリなどリアルタイム伝送が必要なストリームが途切れる可能性がある。この場合、リアルタイム伝送が必要なストリームが途切れない様にするには、伝送データに対して優先制御が必要である。端末だけでなく、ルータやスイッチングハブにおいて、後述するストリーム伝送やファイル転送の速度制限機構などを導入することにより解決できる。たとえば、MPEG-TSストリームの伝送優先度をファイル転送データの伝送優先度よりも高くすると、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG-TSを暗号化してリアルタイムで伝送することが可能となる。

前述したルータ、またはスイッチングハブにおける伝送速度制限機構は、データ流入制御により実現できる。すなわち、ルータ(あるいは、スイッチングハブ)の入力データキューにおいて優先度の高いデータと低いデータを比較して、優先度の高いデータを優先して出力することにより実現できる。この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式自己同期フェアスケジューリング方式WFQ方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。これらのスケジューリング方式に関する情報は、戸田巖著、「ネットワークQoS技術」、平成13年5月25日(第1版)、オーム社刊の第12章などに記述されている。

10

20

30

40

50

(実施の形態 1)

本願第 1 の発明について説明する。図 4 は本願第 1 の発明のパケット送受信手段（機器）に関するブロック図である。401 は A K E 手段を用いた暗号化によるパケット送受信手段である。A K E 手段（402）に対して A K E 設定情報を入力され、この A K E 設定情報に関連した情報、たとえばコピー保護情報と暗号化鍵変更情報、がパケット化手段（403）に入力され、T C P / I P プロトコルのヘッダーを付加され、さらに、フレーム化手段 409 において M A C ヘッダーが付加されイーサネット（R）フレームに変換し、送信フレームとしてネットワークに出力される。ここで、パケット化手段（403）は送信条件設定手段（404）により決定された送信パラメータにより、入力データのパケット化および送信を行なう。なお、送信条件設定管理手段（404）には、A V データのフォーマット情報は、M I M E タイプ、ファイルタイプ、または拡張子のいずれかを含む送信データのフォーマット種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが入力され、パケット化手段（403）およびフレーム化手段（409）で生成するヘッダーやペイロードデータなどを設定する。

【0013】

ここで、送信先アドレスやポート番号の情報などの設定は U P n P フォーラムが規定している U P n P、デバイスアーキテクチャー（たとえば、DA ver.1.0）を参照して利用する。また、U P n P 以外の W E B ブラウザーを利用したアプリケーションや独自のアプリケーションで設定してもよい。

また、A V データのフォーマット情報は、M I M E タイプ、ファイルタイプ、または拡張子のいずれかを含む送信データのフォーマット種別などより構成され、コピー制御情報（C C I）、C o p y C o n t r o l I n f o r m a t i o n などとともに、U P n P フォーラムの規定している U P n P - A V 仕様を参照して設定する。また、U P n P - A V で規定する仕様以外の W E B ブラウザーを利用したアプリケーションや独自のアプリケーションで設定してもよい。

受信側では、ネットワークより入力する信号がフレーム受信手段（410）で M A C ヘッダーを元にフィルタリングされ、I P パケットとしてパケット受信手段（405）に入力される。パケット受信手段（405）では I P パケットヘッダーなどの識別によりフィルタリングを行い、A K E 手段（402）に入力される。これにより送信側の A K E 手段と、受信側の A K E 手段がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージの交換ができる。すなわち、A K E 手段の設定手順に従い、認証と鍵交換を実行することができる。

【0014】

送信側と、受信側で認証と鍵交換が成立すれば、暗号化した A V データを送信する。送信条件設定手段（404）は、この時、A V データのコピー制御情報、およびフォーマット情報により暗号化モードの設定、または、暗号化情報ヘッダー付加の実行の少なくともいずれか一方の動作を、暗号化データ生成手段（406）、およびパケット化手段（403）に対して制御する。

送信側では、M P E G - T S 信号を暗号化手段（406）に入力して、M P E G - T S 信号を暗号化した後、この暗号化された M P E G - T S 信号をパケット化手段（403）に入力し、T C P / I P プロトコルのヘッダーを付加する。さらに、フレーム化手段 409 において、802.1Q（V L A N）方式を用いて、M A C ヘッダーを付加しイーサネット（R）フレームに変換して、送信フレームとしてネットワークに出力する。ここで、M A C ヘッダー内の T C I（Tag Control Information）内の P r i o r i t y（ユーザ優先度）を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

受信側では、ネットワークより入力する信号がフレーム受信手段（410）で M A C ヘッ

ダーを元にフィルタリングされ、IPパケットとしてパケット受信手段(405)に入力される。パケット受信手段(405)でパケットヘッダーなどの識別によりフィルタリングされ、復号手段(407)に入力され、復号されたMPEG-TS信号が出力される。

【0015】

なお、送信条件設定手段(404)には、受信状況を送信側にフィードバックするためのデータが入力され、パケット化手段(403)およびフレーム化手段(409)で生成するヘッダーおよびペイロードデータを設定する。

【0016】

次に、図5のプロトコルスタックを用い上記手順を補足説明する。図5の送信側において、まず送信側から受信側へ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求を送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報(機器ID、機器の認証情報、マックアドレスなど)、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせて生成した情報であり、DES方式やAES方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新報を生成し、受信側に送信する。コンテンツであるMPEG-TSは暗号化鍵により暗号化される。そして暗号化されたMPEG-TSは、1つ以上のTSパケットを単位として前述したEMIなどの暗号化モード情報や、鍵生成の元情報となる数値情報と結合して、伝送AVデータペイロードとしてHTTPやRTPのパケットペイロードとしてマッピングされる。さらにこのHTTPまたはRTPパケットは、TCPまたはUDPプロトコルにマッピングされ、次にIPパケットのデータペイロードとして使用され、IPパケットが生成される。さらにこのIPパケットはMACフレームのペイロードデータとして使用され、イーサネット(R)MACフレームが生成される。なお、MACとしてはイーサネット(R)であるIEEE 802.3だけでなく、無線LAN規格のIEEE 802.11のMACにも適用できる。

【0017】

さて、イーサネット(R)MACフレームは、イーサネット(R)上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット(R)MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからTCP(またはUDP)パケットが抜き出される。そして、TCP(またはUDP)パケットからAVデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、MPEG-TS(コンテンツ)が復号され出力される。

【0018】

以上、MPEG-TS信号などのAVストリームを送信機器で暗号化して、IPパケットをネットワークにより伝送し、受信機器で元の信号に復号することが可能である。

なお、図3において、スイッチングハブを用いたネットワークポロジを工夫することにより、ストリーム伝送とファイル転送を共存させることができる。たとえば、1階と2階の間のネットワーク305の帯域を、従来の実施例で説明した100Mbpsから1Gbpsに拡張することによって、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG-TSを暗号化してリアルタイムで伝送することができる。たとえば、市販されている100Mbpsのポートを8つ、1Gbpsのポートを1つ持ったスイッチングハブを用い、1階と2階を結ぶネットワーク305に1Gbpsのポートを接続し、残りの8chの100MbpsのポートにTVなどのAV機器を接続する。100Mbpsのポートは8つなので、8つのポートのデータがそれぞれ最大100Mbpsで入力されて1G

10

20

30

40

50

b p s のポートに出力されたとしても、 $100\text{Mbps} \times 8\text{ch} = 800\text{Mbps}$ と 1Gbps より小さいため、8つのポートから入力されたデータはスイッチングハブ内部で失われず全て 1Gbps のポートに出力される。よって、1階で発生したデータは全て2階に伝送することが可能である。また、逆に2階で発生したデータも全て1階に伝送することが可能である。以上の様に、スイッチングハブを用いる場合、ネットワークトポロジを工夫することによりストリーム伝送とファイル転送を共存させることができる。

【0019】

なお、AKE および AV データの暗号化方式として D T C P 方式を用いることができる。

。(実施の形態2)

本願第2の発明について説明する。図6は本願第2の発明のブロック図である。図6においては、AKE 手段(402)、および複数の暗号化鍵の保持手段(602)以外は、図4と同様の構成である、よって以下では新規な部分について説明する。

【0020】

本願第2の発明では、第1の発明における暗号化手段におけるAVデータ伝送中の鍵更新において、複数の暗号化鍵から1つの暗号化鍵を選択して暗号化処理を高速実行するために、暗号化鍵は送信手段が持っている暗号化鍵生成用の元データと、複数モードを持つ暗号化制御情報に対応した複数の暗号化鍵をメモリ空間に保持し、送信の暗号化モードが決定の後、複数の暗号化鍵よりその暗号化モードに応じた暗号化鍵を選択して暗号化手段の暗号化鍵を設定し、暗号化を行う。これらの構成により、高速なAVデータを伝送しながら、複数の暗号化鍵から1つの暗号化鍵を選択して鍵更新を高速に行いながら、暗号化処理を高速実行することが可能となる。

図6において、AKE 手段(402)に対してAKE 設定情報を入力され、このAKE 設定情報に関連した情報(たとえば、コピー制御情報と暗号化鍵変更情報)、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段(ローカル)と受信手段(リモート)における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化手段(403)に入力され、T C P / I P プロトコル処理をして、第1キュー手段(603)に入力される。

ここで、送信条件の設定管理手段(404)とAKE 手段(402)は、それぞれ、暗号鍵を生成する情報を与え、AKE 手段(402)で複数の暗号化モード(E M I など)に応じて1つ以上の暗号化鍵生成手段(601)を生成し、複数の暗号化鍵の保持手段(602)にセットする。伝送されるAVデータが暗号化データ生成手段(406)に入力されれば、そのAVデータのコピー制御情報に応じて、複数の暗号化鍵の保持手段(602)にセットされた複数の暗号化鍵より1つの暗号化鍵を選択する。この選択された暗号化鍵は、A E S 方式やD E S 方式などの暗号化手段にセットにAVデータを暗号化し、パケット化手段(403)に出力する。ここで、暗号化鍵生成手段(601)はハードウェア、複数の暗号化鍵の保持手段(602)はソフトウェアのメモリ、暗号化手段はハードウェアの構成を使用することにより、高速で暗号化鍵の更新を行ないながらAVデータの送信が実現できる。

【0021】

受信側の動作は第1の実施例と同様である。

(実施の形態3)

本願第3の発明について説明する。本願第3の発明は、第1の発明における暗号化データ生成手段において、外部入力されるAVストリームのコピー制御情報(C C I)に従うより、M I M E - T Y P E などAVデータのフォーマット情報を暗号化データ仕様のフォーマットに変更をした後、暗号化伝送する。さらに、AVストリームのオリジナルのフォーマット情報をU P n P - A V 方式や独自の通信方式を利用して別のデータにマッピングして、送信側から受信側に伝送する。これらの構成により、AVデータのフォーマット情報を変更して暗号化伝送しながら、受信側でAVデータのオリジナルのフォーマット情報

を復元することが可能となる。

【0022】

図6は本願第3の発明のブロック図である。図6において、AKE手段(402)に対してAKE設定情報を入力し、このAKE設定情報に関連した情報(たとえば、コピー保護情報と暗号化鍵変更情報)、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段(ローカル)と受信手段(リモート)における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが第1の packets 化手段(701)にされプロセッサを用いたソフトウェア処理でTCP/IPプロトコル処理をされ、第1キュー手段(603)にされる。

10

送信条件の設定管理手段(404)には、AVデータのフォーマット情報が入力されている。一方、AVデータのフォーマット情報は、前述した暗号化モード(EMIなど)に応じて、そのフォーマット情報が書き換えられる。たとえば、暗号化しない場合はAVデータのフォーマット情報は、

video/mpegのまま変更しない。また、暗号化する場合はAVデータのフォーマット情報は、video/mpegからapplication/x-dtcp1などに変更する。さらに、video/mpegの付帯情報として、mpeg-ps、mpeg-ts、NTSCやPALなどの情報をAVデータとしてではなく別データとして、UPnP-AVや専用プロトコルなどを使用して送信側から受信側に伝送する。受信側では、受け取った情報から、元のAVデータのフォーマットを復元できる。これらのMIMEタイプはIETFのRFC規格やARIB(電波産業界)の規格などに記述されている。ARIBの規格に記述されている仕様としては、たとえば、
application/x-arib-mpeg-ts
や

20

application/x-arib-mpeg-ts

などがある。

(実施の形態4)

本願第4の発明について説明する。

本願第4の発明は、第1の発明において、AVデータの packets 化は、受信側からの制御により、RTP/UDPまたはHTTP/TCPプロトコルの切替え制御を、きめ細かく、かつ映像の途切れなくスムーズに行う。

30

図9は本願第4の発明のブロック図である。図9の packets 化手段(403)内の第1の packets 化手段(901)および第2の packets 化手段(902)、 packets 受信手段(405)内の第1の packets 受信手段(903)および第2の packets 受信手段(904)を持つ。ここで第1の packets 化手段(901)はRTP方式、第2の packets 化手段(902)はHTTP方式、第1の packets 受信手段(903)はRTP方式、また、第2の packets 受信手段(904)はHTTP方式の packets 処理を行う。

AVデータの packets 化は、受信側から送信側におけるTVチューナのチャンネル選択や、受信側でHDDがDVDディスクに録画されたAVコンテンツの選択コマンドが出された場合には、第1の packets 化手段(901)および第1の packets 受信手段(903)を使用し、伝送遅延の小さいRTP方式で、TVチューナのチャンネル選択や録画されたAVコンテンツの選択を速く行う。また、これらの視聴コンテンツ選択が終了した後は、第2の packets 化手段(902)および第2の packets 受信手段(904)を使用し、HTTP/TCPプロトコルを用い、RTP/UDPよりも packets 落ちに対してTCPでの再送機能を持つHTTP/TCP方式を用いて高画質なコンテンツ視聴を行う。これらの構成により、切替え制御することにより受信側でコンテンツ選択をする場合は低遅延でユーザに遅延を感じさせない軽快な操作が可能となり、また、視聴コンテンツ選択が終了した後は packets ロスなどによる信号欠落が補償された高品質なAVコンテンツの伝送が可能となる。

40

(実施の形態5)

50

本願第5の発明について説明する。図10は本願第5の発明のブロック図である。図10においては、時間情報付加手段(1001)、および時間情報判別手段(1002)以外は、図9と同様の構成である、よって以下では新規な部分について説明する。

【0023】

本願第5の発明は、第1の発明において、AVデータを構成するデータブロックに、タイムスタンプまたは提携データから構成される時間情報を付加し、時間情報を付加した付データブロックを1つ以上まとめてRTPパケットのペイロード部またはH-TTPパケットのペイロード部にマッピングする。これにより、TSパケットにタイムスタンプや特定情報を付加できるので、受信側でMPEG-TSのデコードをタイムスタンプを用いて行うか、タイムスタンプを用いないで用いるかをきめ細かく制御することが可能となる。

10

【0024】

図11は、MPEG-TSをIPパケット化、さらにイーサネット(R)フレーム化して伝送する場合のパケット形式の一例である。188バイトのMPEG-TSに6バイトのタイムコード(TC)を付加して194バイトの単位を作る。TCは42ビットのタイムスタンプと6ビットのベースクロックID(BCID)により構成される。BCIDによりタイムスタンプの周波数情報を表すことができる。たとえば、(ケース1)BCIDが0x00の場合は、タイムスタンプの周波数情報はない、(ケース2)BCIDが0x01の場合は、タイムスタンプの周波数情報としては27MHz(MPEG2のシステムクロック周波数)である、(ケース3)また、BCIDが0x02の場合は、タイムスタンプの周波数情報としては90kHz(MPEG1で使用されるクロック周波数)である、(ケース4)BCIDが0x03の場合は、タイムスタンプの周波数情報としては24.576MHz(IEEE 1394で使用されるクロック周波数)である。(ケース5)BCIDが0x04の場合は、タイムスタンプの周波数情報としては100MHz(イーサネット(R)で使用される周波数)である、という様にBCIDでタイムスタンプの周波数情報を表すことができる。194バイト単位のデータを2つあわせて暗号化して、更に2バイトのD-TCP情報と合わせてRTPプロトコルのペイロードとする。ここで、D-TCP情報は、2ビットのEMIと、1ビットのO/Eと13ビットのReserved Dataにより構成される。RTPパケットはUDPおよびIPプロトコルによりパケット化された後、イーサネット(R)フレーム化される。イーサネット(R)ヘッダとしては、図9に示す様に、標準的なイーサネット(R)ヘッダーとIEEE 802.1Q(VLAN)により拡張されたイーサネット(R)ヘッダーの両方をサポートする。なお、IEEE 802.1Q(VLAN)により拡張されたイーサネット(R)ヘッダーにおけるTCIフィールドの中の3ビットのPriorityフラグにより、イーサネット(R)フレームの優先度を設定することができる。また、受信側でタイムスタンプのある状態とタイムスタンプのない状態を識別するには、UPnP-AVや特定アプリケーションで状態識別フラグを通知する構成をとってもよい。

20

30

【0025】

また、MPEG-TSにARIB-STD-B21で規定された4バイトのタイムコード(TC)を付加して192バイトとしてもよい。この場合、前述した(ケース1)のBCIDが0x00に相当する状態、すなわち、タイムスタンプの周波数情報のない状態として、オール1などある特定の値を定義してタイムスタンプのある状態とタイムスタンプのない状態を規定することができる。

40

【0026】

受信側でタイムスタンプのある状態とタイムスタンプのない状態を識別するには、UPnP-AVや特定アプリケーションで状態識別フラグを通知する構成がとれる。また、4バイトデータとしてオール1などある特定の値の受信値から判別することもできる。

【0027】

なお、上述した実施の形態1から5においては、一般のIPネットワークなどパケットの順序性が保証されていない通信網で伝送する場合には、パケットにシーケンス番号を付加して送信し、受信側でシーケンス番号を用いて順序性の保証を行ってもよい。この順序

50

性の保証は、OSIモデルの第4層以上、すなわち、RTPプロトコルやビデオ信号処理などで行なうことができる。

【0028】

なお、送信側側でハードウェア処理され伝送されたAV信号のパケットが、ネットワークでフラグメントされないため対策ができる。すなわち、送信側において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメントされない最大サイズ(MTU)を検査し、それ以下のパケットサイズで伝送すればよい。あるいは、RFCの規格では全ての端末は576バイトのサイズのIPパケットを扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器はこれ以下のIPパケットではフラグメントが起こらない。したがってIPパケットのサイズが576バイト以下となるように、送信側側でハードウェア処理されるAV信号のパケットサイズを調整すればよい。なお、送信側側でハードウェア処理されるAV信号のパケットにフラグメントが起こらない場合は、受信したパケットがフラグメントされていれば全て一般パケットとして処理すればよい。なお、イーサネット(R)のIPパケットの最大値を越えた場合は送信端末でフラグメントしなければ行けないので、優先パケットのフラグメントを起こさせないためにはIPパケットの最大値以下でなければならないことは言うまでもない。

10

【0029】

また、通信網においてフラグメントが起こる確率が非常に低い場合は、送信側側でハードウェア処理され伝送されたAV信号のパケットのIPヘッダにフラグメント禁止のフラグを立てて伝送することにより、ルータがフラグメントせざるを得ない状態ではIPパケットを廃棄させることにより、受信端末のフラグメント処理負荷を軽減してもよい。この場合、非常に少数のパケットは損失となるが、受信側で誤り訂正あるいは誤り修整を行うことで通信品質を補償することができる。

20

さらに、実施の形態1から実施の形態6までは、通信網プロトコルとしてイーサネット(R)を例としたがこの限りではない。

【0030】

また、ビデオ信号処理の例として、実施の形態1から5ではMPEG-TSを用いたが、これに限らず本発明で用いる入力データの適用範囲としては、MPEG1/2/4などMPEG-TSストリーム(ISO/IEC 13818)、DV(IEC 61834、IEC 61883)、SMPTE 314M(DV-based)、SMPTE 259M(SDI)、SMPTE 305M(SDTI)、SMPTE 292M(HD-SDI)等で規格化されているストリームを含んだあらゆる映像、音声に関するストリームまでも適用可能である。映像や音声のデータレートは、CBR(constant bit rate)に限るものではない。さらに、映像や音声だけでなく、一般のリアルタイムデータ、あるいは優先的に送受信を行うデータであればどのようなものでも本願発明から排除するものではない。

30

また、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、一定の条件化でリアルタイムより高速の伝送も可能である。

【図面の簡単な説明】

40

【0031】

【図1】本願第1の発明を適用するシステムの一例を示す図

【図2】認証と鍵交換にDTCP方式を適用する場合のコンテンツ伝送手順の説明図

【図3】イーサネット(R)を用いる一般家庭に適用した場合の一例の説明図

【図4】本願第1の発明のパケット送受信手段(機器)のブロック図

【図5】本願第1の発明のプロトコルスタックによる説明図

【図6】本願第2の発明のパケット送受信手段のブロック図

【図7】本願第3の発明のパケット送受信手段のブロック図

【図8】本願第3の発明のプロトコルスタックによる説明図

【図9】本願第4の発明のパケット送受信手段のブロック図

50

【図10】本願第5の発明の packets 送受信手段のブロック図

【図11】本願第5の発明における MPEG-TS のイーサネット (R) フレーム構成仕様の例を示す図

【図12】DTCP方式を用いた MPEG-TS の IEEE 1394 での伝送の一例を示す図

【図13】DTCP方式における従来の packets 通信手段の概略説明図

【図14】IEEE 1394 において DTCP を用いた暗号化ストリーム伝送手順を示す図

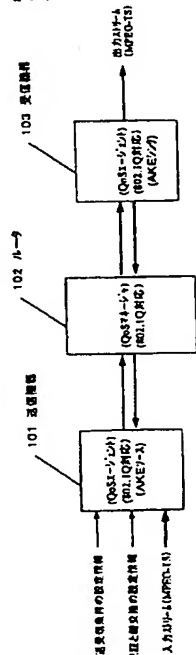
【図15】MPEG-TS 信号を伝送する場合の IEEE 1394 アイソクロナス packets の一例を示す図

【符号の説明】

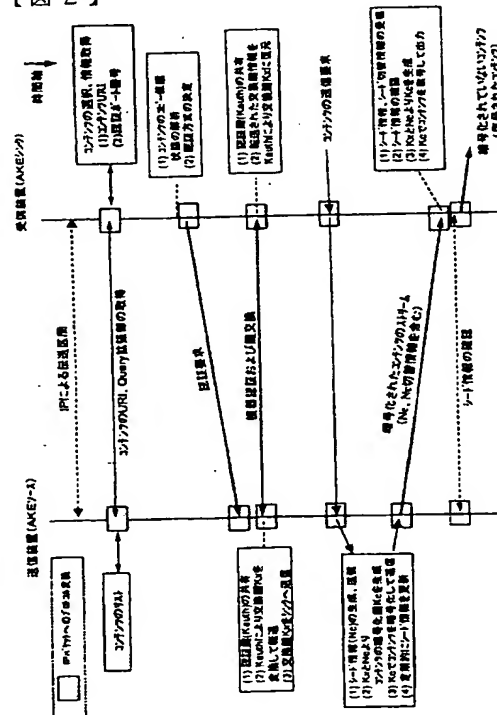
【0032】

- 101 パケット送信機器
- 102 ルータ
- 103 パケット受信機器
- 401 パケット送受信手段 (機器)
- 402 AKE 手段
- 403 パケット化手段
- 404 送信条件の設定管理手段
- 405 パケット受信手段
- 406 暗号化手段
- 407 復号手段
- 408 受信条件の設定管理手段
- 409 フレーム化手段
- 410 フレーム受信手段

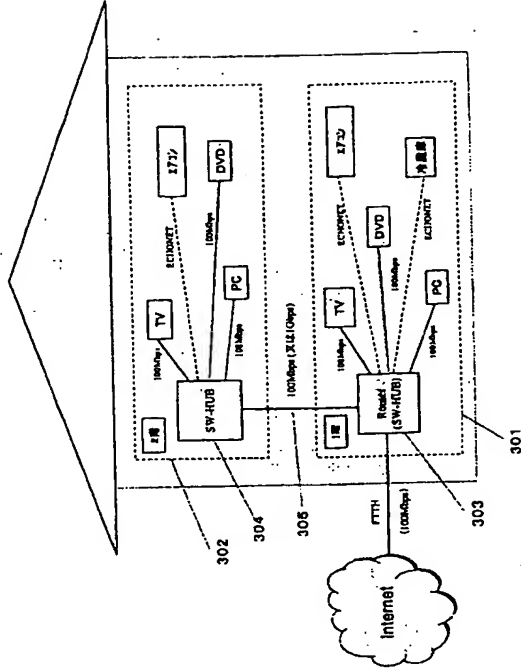
【図1】



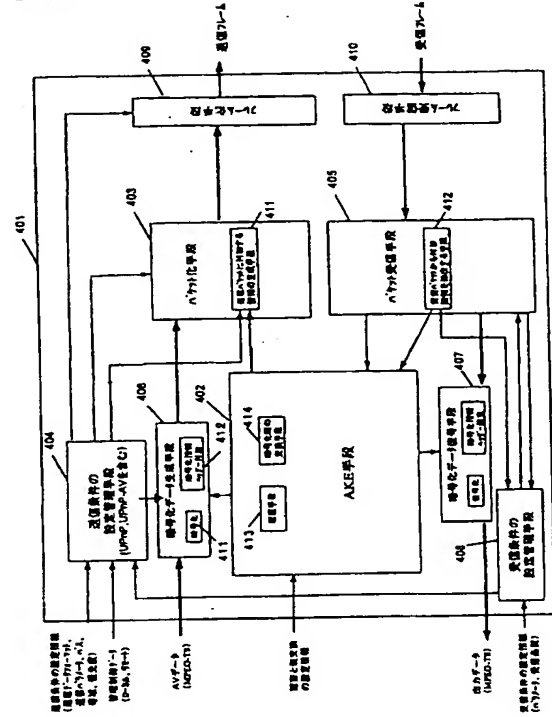
【図2】



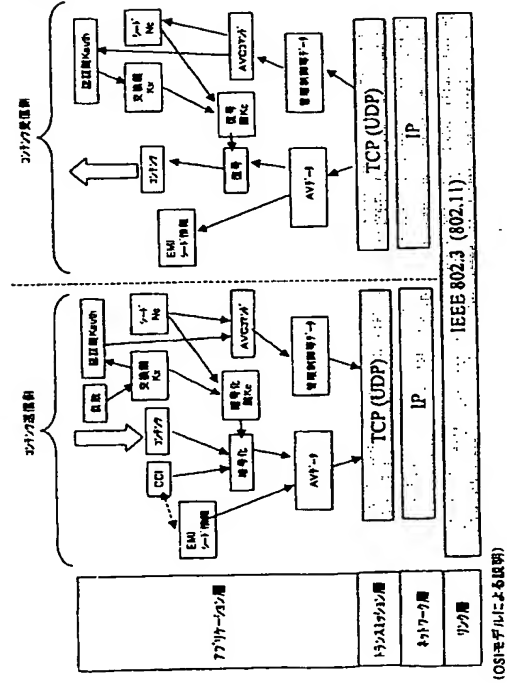
【 図 3 】



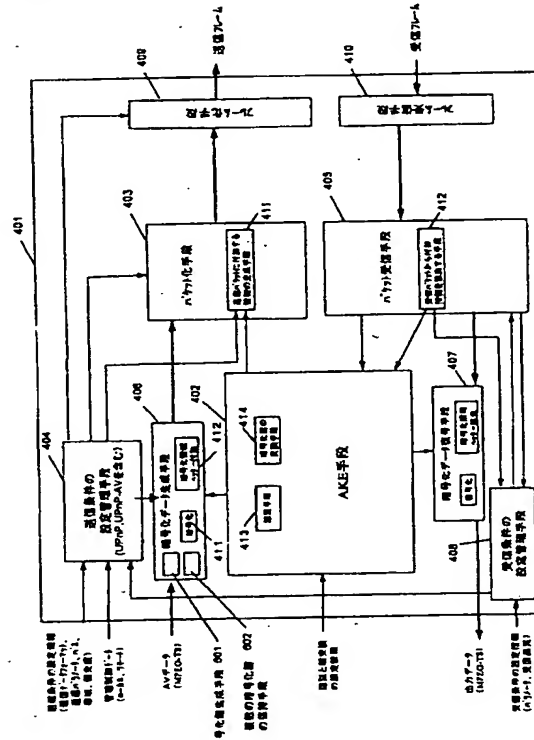
【 ㊦ 4 】



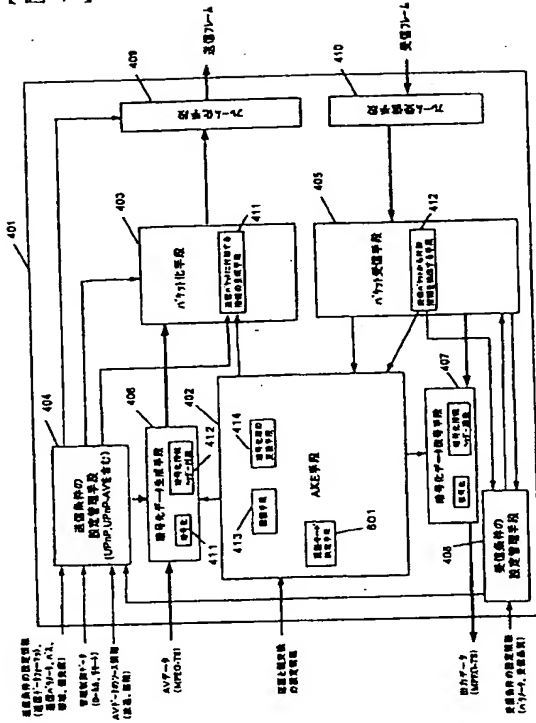
【圖 5】



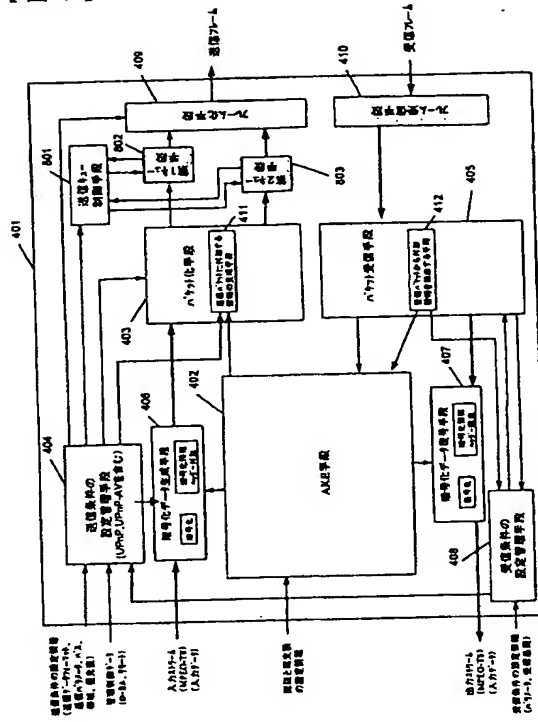
【図 6】



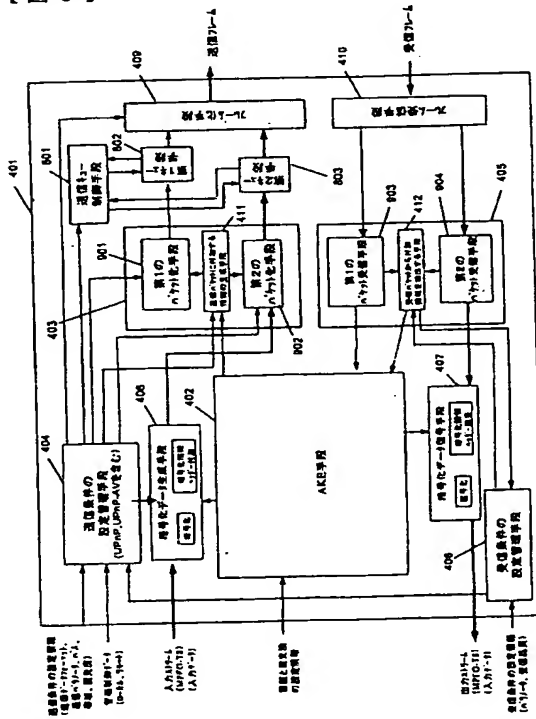
【図 7】



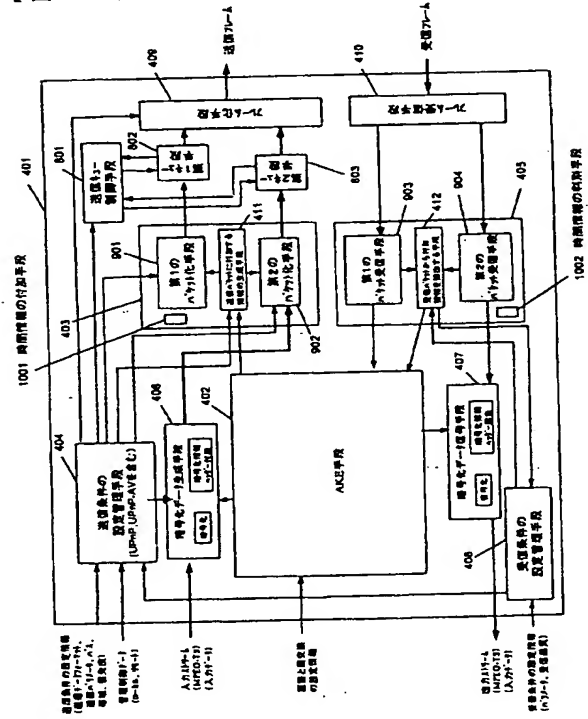
【図 8】



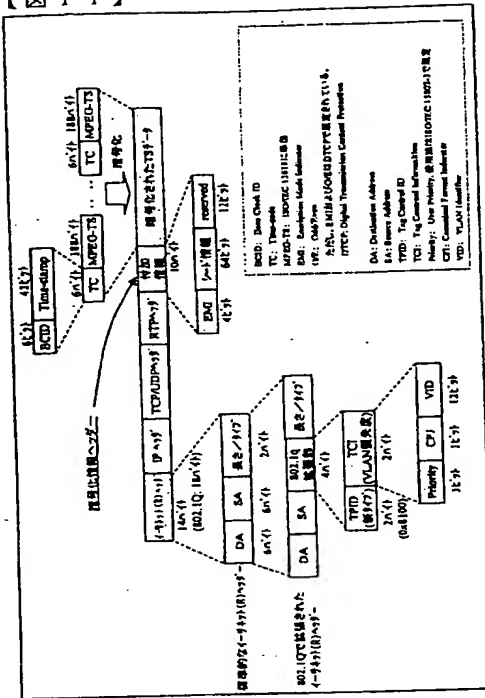
【図 9】



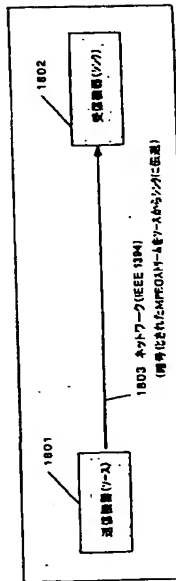
【図 10】



【☒ 1 1】



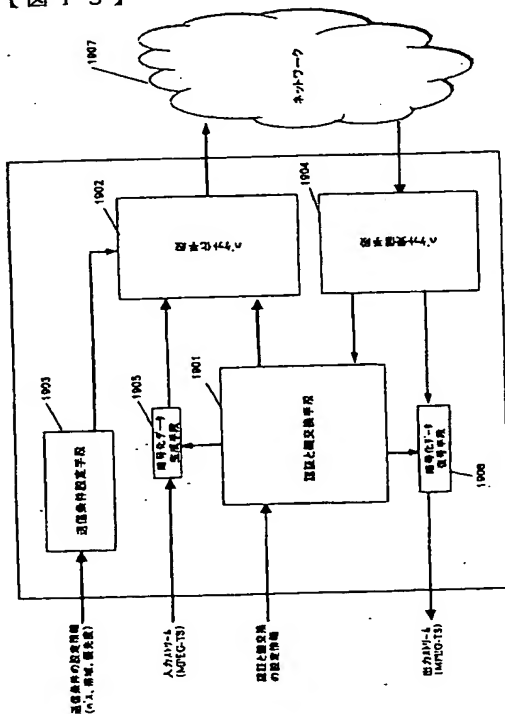
【 1 2 】



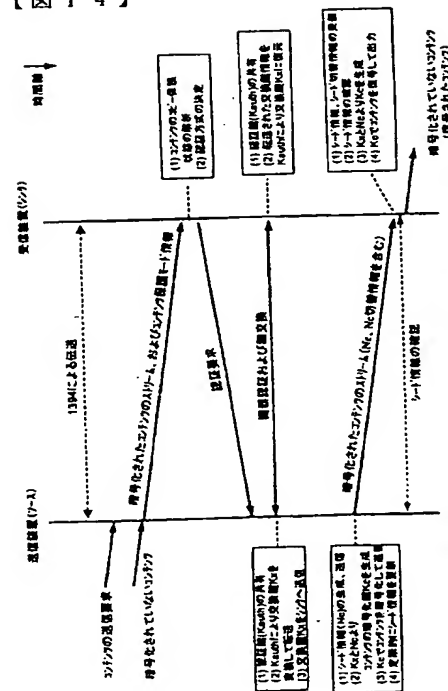
液晶ディスプレイの例	液晶ディスプレイの例	液晶ディスプレイの例
DMS	DMS	DMS
HDD-3+1	HDD-3+1	HDD-3+1
1304画素GTG	1304画素GTG	1304画素GTG
1304画素TFT/STN	1304画素TFT/STN	1304画素TFT/STN

THE 1994 において DTCF を用いた MPEQAL への応用

【 ㊦ 1 3 】



【图 14】



TEEE 1394においてDICPを用いた増量化スリッサー伝送系(健康版)

[illegible]

フロントページの続き

(51)Int.Cl.⁷

F I

テーマコード (参考)

H 0 4 N 7/16

(72)発明者 臼木 直司

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

Fターム(参考) 5C025 AA01 AA30 BA27 DA01 DA08

5C063 AB03 AB05 AC10 DA07 DA13

5C064 BA01 BB02 BC16 BC17 BC20 BC22 CA14 CB01 CC04

5J104 AA01 AA12 AA16 EA04 EA16 EA18 JA03 NA02 NA37 PA01

PA05 PA07